THAT WHICH IS CLAIMED IS:

1. A cryptographic device comprising:

an input stage receiving an input data block and a key data block comprising a plurality of sub-key data blocks, and generating a plurality of first signals therefrom;

an intermediate stage connected to said input stage and comprising

a plurality of substitution units, each substituting data within a respective first signal, and

a diffuser connected to said plurality of substitution units for mixing data to generate a diffused signal; and

an output stage connected to said intermediate stage for repetitively looping back the diffused signal to said input stage for combination with a next sub-key data block.

2. A cryptographic device according to Claim 1 wherein the looping back is repeated a predetermined number of times; and wherein said output stage provides an output signal for the cryptographic device after the repetitively looping back is complete.

3. A cryptographic device according to Claim 2 wherein the output signal is further combined with a final sub-key data block.

4. A cryptographic device according to

Claim 1 wherein each substitution unit performs a non-linear substitution based upon at least one look-up table.

5. A cryptographic device according to Claim 1 wherein said diffuser comprises a shift register and a look-up table associated therewith.

6. A cryptographic device according to Claim 1 wherein said diffuser comprises a plurality of shift registers and a plurality of look-up tables associated therewith.

7. A cryptographic device according to Claim 1 wherein said output stage performs a row-shift operation on the diffused output signal before being looped back to said input stage.

8. A cryptographic device according to Claim 1 wherein said output stage performs a column-mix operation on the diffused output signal being looped back to said input stage.

9. A cryptographic device according to Claim 1 wherein said output stage comprises a counter for counting a number of times the diffused output signal is looped back to said input stage.

10. A communication system comprising:

a key scheduler providing a key data block comprising a plurality of sub-key data blocks; and

a cryptographic device connected to said key scheduler and comprising

an input stage receiving an input data block and the key data block, and generating a plurality of first signals therefrom;

an intermediate stage connected to said input stage and comprising

a plurality of substitution units, each substituting data within a respective first signal, and

a diffuser connected to said plurality of substitution units for mixing data to generate a diffused signal, and

an output stage connected to said intermediate stage for repetitively looping back the diffused signal to said input stage for combination with a next sub-key data block, said output stage providing an output signal for the cryptographic device after the repetitively looping back is complete.

11. A communication system according to Claim 10 wherein the output signal is further combined with a final sub-key data block.

12. A communication system according to Claim 10 wherein each substitution unit performs a non-linear substitution based upon at least one look-up table.

13. A communication system according to

Claim 10 wherein said diffuser comprises a shift register and a look-up table associated therewith.

14. A communication system according to Claim 10 wherein said diffuser comprises a plurality of shift registers and a plurality of look-up tables associated therewith.

15. A communication system according to Claim 10 wherein said output stage performs a row-shift operation on the diffused output signal before being looped back to said input stage.

16. A communication system according to Claim 10 wherein said output stage performs a column-mix operation on the diffused output signal being looped back to said input stage.

17. A communication system according to Claim 10 wherein said output stage comprises a counter for counting a number of times the diffused output signal is looped back to said input stage.

18. A method for converting an input data block into an output signal in a cryptographic device, the method comprising:

generating a plurality of first signals based upon the input data block and a key data block comprising a plurality of sub-key data blocks;

substituting data within each first signal using a respective substitution unit;

mixing data to generate a diffused signal using a diffuser connected to the respective substitution units; and

repetitively looping back the diffused signal for combination with a next sub-key data block before repeating the substituting and mixing.

19. A method according to Claim 18 wherein the looping back is repeated a predetermined number of times; and further comprising providing an output signal for the cryptographic device after the repetitively looping back is complete.

20. A method according to Claim 19 further comprising combining the output signal with a final sub-key data block.

21. A method according to Claim 18 wherein each substitution unit performs a non-linear substitution based upon at least one look-up table.

22. A method according to Claim 18 wherein the diffuser comprises a shift register and a look-up table associated therewith.

23. A method according to Claim 18 wherein the diffuser comprises a plurality of shift registers and a plurality of look-up tables associated therewith.

24. A method according to Claim 18 further comprising performing a row-shift operation on the diffused output signal before being looped back.

25. A method according to Claim 18 further comprising performing a column-mix operation on the diffused output signal being looped back.

26. A method according to Claim 18 further comprising counting a number of times the diffused output signal is looped back.